Quasi-symmetric designs related to the triangular graph

Haemers, W.H.; Coster, M.J.

Published in:
Designs Codes and Cryptography

Publication date:
1995

Designs, Codes and Cryptography, 5, 27–42 (1995)

Quasi-Symmetric Designs Related to the Triangular Graph

M. J. COSTER AND W. H. HAEMERS
Tilburg University, Department of econometrics, P.O. Box 90153, 5000 LE, Tilburg, The Netherlands

Communicated by: D. Jungnickel

Received April 13, 1993; Accepted March 22, 1994

Abstract. Let T_m be the adjacency matrix of the triangular graph. We will give conditions for a linear combination of T_m, I and J to be decomposable. This leads to Bruck-Ryser-Chowla like conditions for, what we call, triangular designs. These are quasi-symmetric designs whose block graph is the complement of the triangular graph. For these designs our conditions turn out to be stronger than the known non-existence results for quasi-symmetric designs.

1. Triangular Designs

A 2–(v, k, λ) design $\mathcal{D}$ (with b blocks and r blocks through a given point) is called *quasi-symmetric* if the sizes of the intersection of two distinct blocks take only two values x and y $(x < y)$, say. The *block graph* Γ of $\mathcal{D}$ is the graph defined on the blocks of $\mathcal{D}$, two vertices being adjacent whenever the blocks meet in y points. S.S. Shrikhande and Bhagwandas [20] (see also Goethals and Seidel [12]) showed that Γ is strongly regular having eigenvalues

$$\left[\frac{kr - k - bx + x}{y - x}\right]^1, \left[\frac{r - k - \lambda + x}{y - x}\right]^{v-1}, \left[\frac{x - k}{y - x}\right]^{b-v} \tag{1}$$

(exponents indicate the corresponding multiplicities). Note that the complement of $\mathcal{D}$ has block intersection sizes $v - 2k + x$ and $v - 2k + y$, and hence has the same block graph as $\mathcal{D}$. The question which strongly regular graphs are block graphs of quasi-symmetric designs is a difficult one and there is no hope for a general answer. The question is already difficult for a simple family of strongly regular graphs, the so-called triangular graphs and their complements. The triangular graph $\mathcal{T}_m$ is the line graph of the complete graph K_m $(m \geq 3)$. It can also be defined as the block graph of the pair design on m points (this is the 2–$(m, 2, 1)$ design whose blocks are just all unordered pairs of points). We denote the complement of $\mathcal{T}_m$ by $\mathcal{T}_m^c$ and write T_m and T_m^c for the corresponding adjacency matrices (so $T_m^c = J - I - T_m$, wherein, as usual, I is the identity and J is the all-one matrix). The eigenvalues of T_m are

$$\left[\ 2m - 4\ \right]^1, \left[\ m - 4\ \right]^{m-1}, \left[\ -2\ \right]^{\binom{m-1}{2}-1}, \tag{2}$$

and those of $\mathcal{T}_m^c$ are

$$\left[\ \binom{m-2}{2}\ \right]^1, \left[\ 3-m\ \right]^{m-1}, \left[\ 1\ \right]^{\binom{m-1}{2}-1}. \tag{3}$$

(Note that (2) follows from (1) applied to the pair design.) The following result is given implicitely in Cameron and Van Lint [6] (our reference is to the latest edition, though the result we refer to was already treated in the very first edition of 1975).

PROPOSITION 1.1 *The block graph of a quasi-symmetric 2–(v, k, λ) design $\mathcal{D}$ is $\mathcal{T}_m$, if and only if $\mathcal{D}$ is the pair design or the complement.*

Proof: The 'if' part is by definition. To prove 'only if', take without loss of generality $k \geq v/2$. By (1) and (2) $\mathcal{D}$ has $\binom{m}{2}$ blocks and m points. Hence by (1.52) to (1.54) of [6], $\mathcal{D}$ is the complement of the unique 4–(23, 7, 1) design, or has $k = v - 2$. For the first possibility the block graph is not $\mathcal{T}_m$ (as follows easily from Formula (1)) and in the second case $\mathcal{D}$ is the complement of the pair design. ■

For $\mathcal{T}_m^c$ the situation is less simple. Proposition 1.2 gives a parameter condition.

PROPOSITION 1.2 *The block graph of a quasi-symmetric 2–(v, k, λ) design $\mathcal{D}$ is $\mathcal{T}_m^c$, if and only if the parameters of $\mathcal{D}$ satisfy*

$$v = \binom{m-1}{2}, b = \binom{m}{2}, k = \tfrac{1}{2}a(m-2), r = \frac{1}{2}am,$$
$$\lambda = \frac{a(am-2a-2)}{2(m-3)}, x = \binom{a}{2}, y = \frac{a(am-4a+2)}{2(m-3)},$$

for some integer a.

Proof: Suppose the block graph of $\mathcal{D}$ is $\mathcal{T}_m^c$. Put $a = r - k$. Then the formulas readily follow by use of Formulas (1) and (3). Conversely, it follows that the block graph of a design with the above parameters has the eigenvalues of $\mathcal{T}_m^c$. For $m \neq 8$ Hoffman [16] and Chang [8] showed that $\mathcal{T}_m^c$ is determined by its eigenvalues. If $m = 8$, a can only be 2 or 6 and so $\mathcal{D}$ is a 2–(21, 6, 2) design or the complement, and such designs do not exist due to Connor [9]. ■

Designs with the parameters of Proposition 1.2 will be called *triangular designs*. If $a = 2$ they are the residual designs of biplanes. Note that replacing a by $m - a - 1$ leads to the complementary parameter set.

In this paper we will derive Bruck-Ryser-Chowla type conditions for the existence of triangular designs using rational decomposability of related matrices. (For a proof of the Bruck-Ryser-Chowla theorem itself by these techniques we refer to Beth Jungnickel and Lenz [2] or Lander [17].) Our main result strengthens an earlier necessary condition for the existence of triangular designs by the second author [13]. This condition (and many other results on quasi-symmetric designs) can also be found in the recent monograph by M. S. Shrikhande and S. S. Sane [19] (p. 147).

M. S. Shrikhande kindly pointed out to us that S. S. Shrikhande, D. Raghavarao and S. K. Tharthare [21] obtained conditions of a similar nature for several types of partial balanced incomplete block designs, including the duals of triangular designs, by use of Hasse-Minkowski invariants. (They use the name triangular design for (the duals of) a more general class of designs.) Their Theorem 5.1 leads to the same conditions for triangular designs as we have.

2. Decomposability

A matrix M is *decomposable* if $M = QQ^{\top}$ for some rational matrix Q. For M to be decomposable, M clearly must be rational, positive semi-definite and the determinant of M has to be rational square. But there are more restrictions. If M has an easy structure, these additional restrictions can often be expressed in terms of some Diophantine equations. The neccessary condition of Bruck, Ryser and Chowla for the existence of a symmetric 2–(v, k, λ) design is based on the fact that $(k-\lambda)I_v + \lambda J$ (the index of I indicates the size) is decomposable. We will derive decomposability conditions for a matrix of the form $\alpha I + \beta T_m + \gamma J$, which will lead to the announced neccessary conditions for triangular designs. In order to do so we need to quote some results on rational congruences. We use the approach and notations of Coster [11], which we will briefly explain.

Let $\mathcal{S}$ be the set of positive definite symmetric rational matrices, including the empty set element. For A, $B \in \mathcal{S}$, we define

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

Let A and B be two elements of $\mathcal{S}$ of dimensions m and n respectively. We say $A \cong B$ (A is congruent to B) if there exists a rational $k \times k$ matrix Q such that $Q(A \oplus I_{k-m})Q^{\top} = B \oplus I_{k-n}$. The relation $\cong$ is an equivalence relation and the operation $\oplus$ acts on the equivalence classes. It can be shown that $(\mathcal{S}/\cong, \oplus)$ is a group. (See [7], [11]. The result is based on Witt's cancellation law. The group is called the Grothendieck Group.) We denote the equivalence class of A by $\langle A\rangle$ and the inverse of $\langle A\rangle$ by $\ominus\langle A\rangle$. Thus $\langle I\rangle = \langle\emptyset\rangle = \langle 1\rangle = 0$. Each class $\langle A\rangle$ can be written as $\langle A\rangle = \sum\langle a_i\rangle = \langle a_1\rangle \oplus \langle a_2\rangle \oplus \cdots$, for some positive integers $a_1, a_2, \ldots$. We denote $\sum_{i=1}^{k}\langle a\rangle$ $(= \langle aI_k\rangle)$ by $k\langle a\rangle$. Note that a matrix $A \in \mathcal{S}$ is decomposable if and only if $\langle A\rangle = 0$.

By $\Box$ we will denote an integral square, and by n^* we denote the squarefree part of an integer n. We denote by $\mathcal{N}_{-1}$ the set of positive integers n with prime factorisation $n = 2^k \prod_i p_i^{k_i} \prod_j q_i^{2l_j}$ with $p_i \equiv 1 \bmod 4$ and k, k_i and l_j non-negative integers. We denote by $\mathcal{N}_2$ the set of positive integers n with prime factorisation $n = 2^k \prod_i p_i^{k_i} \prod_j q_i^{2l_j}$ with $p_i \equiv 1, 7 \bmod 8$ and k, k_i and l_j non-negative integers. We denote by $\mathcal{N}_{-2}$ the set of positive integers with primefactorisation $n = 2^k \prod_i p_i^{k_i} \prod_j q_i^{2l_j}$ where with $p_i \equiv 1, 3 \bmod 8$ and k, k_i and l_j non-negative integers. (We choose the indices -1, 2 and -2 since the Jacobi symbols $\left(\frac{-1}{n}\right)$, $\left(\frac{2}{n}\right)$ and $\left(\frac{-2}{n}\right)$ are equal to 1 for the respective values of n.) The following lemma gives some basic congruences.

LEMMA 2.1 *Let a, b and c be positive rational numbers, then*

(1) $\langle ab^2\rangle = \langle a\rangle$,

(2) $\langle a\rangle \oplus \langle b\rangle = \langle a+b\rangle \oplus \langle ab(a+b)\rangle$,

(3) $2\langle (a^2+b^2)c\rangle = 2\langle c\rangle$,

(4) $4\langle a\rangle = 0$,

(5) $\langle aI_c + \frac{b-a}{c}J\rangle = c\langle a\rangle \ominus \langle ac\rangle \oplus \langle bc\rangle$.

Proof: Property (**1**) is obvious and implies that a, b and c may assumed to be integers. To prove (**2**), define

$$Q = \begin{pmatrix} 1 & 1 \\ -b & a \end{pmatrix},$$

then $Q(\langle a\rangle \oplus \langle b\rangle)Q^{\top} = \langle a+b\rangle \oplus \langle ab(a+b)\rangle$. Congruence (**3**) follows from (**1**) and (**2**): $2\langle c\rangle = \langle a^2c\rangle \oplus \langle b^2c\rangle = 2\langle (a^2+b^2)c\rangle$. To prove (**4**) we use Lagrange's theorem (see [15]) and write $a = b^2+c^2+d^2+e^2$ for integers b, c, d and e. We assume $b^2+c^2>0$ and $d^2+e^2>0$ (otherwise (**4**) follows directly from (**1**) or (**3**)). Then we find by use of (**2**) and (**3**): $0 = 2\langle b^2+c^2\rangle \oplus 2\langle d^2+e^2\rangle = 2\langle b^2+c^2+d^2+e^2\rangle \oplus 2\langle (b^2+c^2)(d^2+e^2)(b^2+c^2+d^2+e^2)\rangle = 4\langle a\rangle$. To prove (**5**) define

$$Q = \begin{pmatrix} -I_{c-1} & \underline{1} \\ \underline{1}^{\top} & 1 \end{pmatrix}$$

($\underline{1}$ is the all-one vector). Then

$$Q(aI_c + \frac{b-a}{c}J)Q^{\top} = (aI_{c-1} + aJ) \oplus \langle bc\rangle.$$

For $a=b$ this yields $\langle aI_{c-1}+aJ\rangle = c\langle a\rangle \ominus \langle ac\rangle$. Hence $\langle aI_c + \frac{b-a}{c}J\rangle = c\langle a\rangle \ominus \langle ac\rangle \oplus \langle bc\rangle$. ∎

Next we quote some lemmas that relate congruences to properties of the involved integers. Most results can be found in [10] or [11]. For Lemma 2.6 we refer to [18], pp. 160–161.

LEMMA 2.2 *Let a, b and c be positive integers which are squarefree and relatively prime in pairs. Then the following three statements are equivalent:*

(1) $\langle ac\rangle \oplus \langle bc\rangle = \langle ab\rangle$,

(2) $aX^2+bY^2 = cZ^2$ *has a non trivial integral solution in X, Y and Z,*

(3) For all primes p dividing a the Legendre symbol $\left(\frac{bc}{p}\right) = 1$, for all primes q dividing b, $\left(\frac{ac}{q}\right) = 1$ and for all primes r dividing c, $\left(\frac{-ab}{r}\right) = 1$.

LEMMA 2.3 *Let a, b and c be positive integers which are squarefree and relatively prime in pairs. Then the following three statements are equivalent:*

(1) $\langle ab\rangle \oplus \langle ac\rangle \oplus \langle bc\rangle = 0$.

(2) $aX^2+bY^2+cZ^2 = abcW^2$ has an integral solution in X, Y, Z and W with $XYZ \neq 0$,

(3) For all primes p dividing a, $\left(\frac{-bc}{p}\right) = 1$, For all primes q dividing b, $\left(\frac{-ac}{q}\right) = 1$, For all primes r dividing c, $\left(\frac{-ab}{r}\right) = 1$.

LEMMA 2.4 *Let a, b and c be integers which are squarefree and relatively prime in pairs. And suppose that $\langle ab\rangle \oplus \langle ac\rangle = \langle bc\rangle$. Then either:*

(1) abc is odd and $a \equiv b \bmod 4$ or $a \equiv c \bmod 4$,

(2) a is even and $b + c \equiv 0 \bmod 8$ or $b + c \equiv 0 \bmod 8$,

(3) bc is even, say b is even and $b + c \equiv a \bmod 8$ or $a \equiv c \bmod 8$.

LEMMA 2.5 *Let a, b and c be integers which are squarefree and relatively prime in pairs. And suppose that $\langle ab\rangle \oplus \langle ac\rangle \oplus \langle bc\rangle = 0$. Then either:*

(1) abc is odd and $a \equiv b \equiv c \bmod 4$,

(2) abc is even and $a + b + c \equiv 4 \bmod 8$,

(3) abc is even, say a is even and $b + c \equiv 4 \bmod 8$.

LEMMA 2.6 *For $i = -2, -1, 2$ we have*

$$X^2 - iY^2 = nZ^2 \text{ has an integral solution for } X,\ Y \text{ and } Z \Leftrightarrow n \in \mathcal{N}_i.$$

3. The Results

In this section we state the main theorems. The proofs are postponed to the next section. The first result gives a decomposability condition for a matrix of the form

$$\mathbb{T}_m = \alpha I + \beta T_m + \gamma J.$$

Using the eigenvalues of T_m, we find that the eigenvalues of $\mathbb{T}_m$ are

$$\begin{aligned} r_0 &= \alpha + 2\beta(m-2) + \tfrac{1}{2}\gamma m(m-1), \\ r_1 &= \alpha + \beta(m-4), \\ r_2 &= \alpha - 2\beta, \end{aligned}$$

with multiplicities 1, $m-1$ and $\binom{m-1}{2}-1$, respectively. We regard $\mathbb{T}_m$ as a function of r_0, r_1 and r_2, rather than α, β and γ and write $\mathbb{T}_m = \mathbb{T}_m(r_0, r_1, r_2)$. The main tool is a diagonal form for $\mathbb{T}_m(r_0, r_1, r_2)$.

THEOREM 3.1

$$\begin{aligned} \langle \mathbb{T}_m(r_0, r_1, r_2)\rangle = \langle r_0\tbinom{m}{2}\rangle \oplus m\langle r_1(m-2)\rangle \ominus \langle r_1 m(m-2)\rangle \\ \oplus \left(\tbinom{m}{2}-1\right)\langle r_2\rangle \oplus \langle 2r_2\rangle \ominus m\langle r_2(m-2)\rangle \oplus \langle 2r_2(m-2)\rangle \ominus \langle 2r_2(m-1)\rangle. \end{aligned} \tag{4}$$

Next we give the necessary condition for the existence of triangular designs.

THEOREM 3.2 *Consider a triangular design with parameters m and a. Let* $\tau = \frac{a(m-a-1)}{2(m-3)}$. *Then*

(1) τ *is integral,*

(2) $(m-2)^{\binom{m}{2}}\tau^{\binom{m+1}{2}}$ *is an integral square,*

(3) $\langle\binom{m-1}{2}\rangle \oplus \left(\binom{m}{2}-1\right)\langle\tau(m-2)\rangle \oplus \langle 2\tau(m-1)\rangle \ominus m\langle\tau\rangle = 0.$

Condition (2) was the main result of [13]. Condition (3) is the main new result of the present paper. The conditions of Theorem 3.2 are made more explicit in the following corollary.

COROLLARY 3.3 *Given a triangular design as in Theorem 3.2.*

(i) If $m \equiv 0 \bmod 8$, *then* $\tau X^2 + (m-2)Y^2 = 2(m-1)Z^2$ *has a non trivial integral solution in X, Y and Z and if* $m \equiv 8 \bmod 16$ *then* τ^* *must be even,*

(ii) if $m \equiv 1 \bmod 8$, *then* $\tau = \square$ *and* $m-2 \in \mathcal{N}_2$,

(iii) if $m \equiv 2 \bmod 4$, *then* $\tau(m-2) = \square$ *and* $m-1 \in \mathcal{N}_{-1}$,

(iv) if $m \equiv 3 \bmod 8$, *then* $m-2 = \square$ *and* $\tau X^2 + Y^2 = 2(m-1)Z^2$ *must have a non trivial integral solution, if* $m \equiv 11 \bmod 16$ *then* τ^* *must be odd,*

(v) if $m \equiv 4 \bmod 8$, *then* $m \equiv 4 \bmod 16$, τ^* *is odd and* $2\tau X^2 + (m-1)Y^2 + \frac{1}{2}(m-2)Z^2 = \tau(m-1)(m-2)W^2$ *has an integral solution in X, Y, Z and W with* $XYZ \neq 0$,

(vi) if $m \equiv 5 \bmod 8$, *then* $\tau = \square$ *and* $m-2 \in \mathcal{N}_{-2}$,

(vii) $m \not\equiv 7 \bmod 8$.

4. The Proofs

To prove Theorem 3.1 we use the following lemma.

LEMMA 4.1

$$\mathbb{T}_m(r_0, r_1, r_2) \cong \left[\frac{r_1}{m-2} I_{m-1} + \frac{r_1(m-4)}{m(m-2)} J\right] \oplus \mathbb{T}_{m-1}\left(\frac{r_0(m-2)}{m}, \frac{r_2}{m-2}, r_2\right).$$

Proof: Define

$$\begin{aligned} E_0 &= \mathbb{T}_m(1,0,0) = \tfrac{2}{m(m-1)} J, \\ E_1 &= \mathbb{T}_m(0,1,0) = \tfrac{1}{m-2}(T_m + 2I - \tfrac{4}{m} J), \\ E_2 &= \mathbb{T}_m(0,0,1) = \tfrac{-1}{m-2}(T_m + (m-4)I - \tfrac{2}{m-1} J). \end{aligned}$$

Then $E_i^2 = E_i$, $E_i E_j = 0$ if $i \neq j$, and $\mathbb{T}_m(r_0, r_1, r_2)E_i = r_i E_i$ (that is, the columns (and rows) of E_i are eigenvectors for the eigenvalue r_i) for $i = 0, 1, 2$. Thus the matrices E_0, E_1 and E_2 are the minimal idempotents of the triangular association scheme, see [6]. We partition the columns of these idempotents according to the partition of $\mathcal{T}_m$ into an $(m-1)$–clique and $\mathcal{T}_{m-1}$: $E_i = \left[\ E'_i \ \ \tilde{E}_i\ \right]$, and we define $Q = \left[\ E'_1 \ \ \tilde{E}_2 + \tilde{E}_0\ \right]$. Then

$$\begin{aligned} Q^{\mathrm{T}}\mathbb{T}_m(r_0, r_1, r_2)Q &= \left[r_1 E'^T_1 E'_1\right] \oplus \left[r_2 \tilde{E}_2^T \tilde{E}_2 + r_0 \tilde{E}_0^T \tilde{E}_0\right] \\ &= \left[\frac{r_1}{m-2}((J - I_{m-1}) + 2I_{m-1} - \frac{4}{m} J)\right] \\ &\quad \oplus \left[\frac{-r_2}{m-2}\left(T_{m-1} - (m-4)I_{\binom{m-1}{2}} - \frac{2}{m-1} J\right) + \frac{2r_0}{m(m-1)} J\right] \\ &= \left[\frac{r_1}{m-2} I_{m-1} + \frac{r_1(m-4)}{m(m-2)} J\right] \oplus \mathbb{T}_{m-1}\left(\frac{r_0(m-2)}{m}, \frac{r_2}{m-2}, r_2\right). \quad \blacksquare \end{aligned}$$

Proof of Theorem 3.1. We use induction on m. By use of **(1)** to **(4)** of Lemma 2.1 we find that for $m = 3$ the right hand side of formula 4 becomes $\langle 3r_0\rangle \oplus 3\langle r_1\rangle \ominus \langle 3r_1\rangle$. On the other hand we have

$$\mathbb{T}_3(r_0, r_1, r_2) = r_1 I + \tfrac{1}{3}(r_0 - r_1) J,$$

which is, by **(5)** of Lemma 2.1, congruent to $3\langle r_1\rangle \ominus \langle 3r_1\rangle \oplus \langle 3r_0\rangle$.
Suppose $m > 3$. Now by Lemma 4.1 and the induction hypothesis we have

$$\begin{aligned} \langle \mathbb{T}_m(r_0, r_1, r_2)\rangle &= \langle \tfrac{r_1}{m-2} I_{m-1} + \tfrac{r_1(m-4)}{m(m-2)} J\rangle \\ &\quad \oplus \langle 2r_0(m-2)^2(m-1)/m\rangle \oplus (m-1)\langle r_2(m-3)/(m-2)\rangle \ominus \\ &\quad \langle r_2(m-1)(m-3)/(m-2)\rangle \oplus (\tbinom{m-1}{2} - 1)\langle r_2\rangle \oplus \langle 2r_2\rangle \ominus \\ &\quad (m-1)\langle r_2(m-3)\rangle \oplus \langle 2r_2(m-3)\rangle \ominus \langle 2r_2(m-2)\rangle. \end{aligned}$$

By use of Lemma 2.1 the first term of the right hand side equals

$$(m-1)\langle r_1(m-2)\rangle \ominus \langle r_1(m-1)(m-2)\rangle \oplus \langle r_1(m-1)(m-2)(m-3)\rangle$$

$$= m\langle r_1(m-2)\rangle \ominus \langle r_1 m(m-2)\rangle,$$

and the remaining part equals

$$\begin{aligned}
&\langle r_0\tbinom{m}{2}\rangle \oplus \langle 2r_2\rangle \oplus (m-1)\langle r_2(m-2)(m-3)\rangle \ominus (m-1)\langle r_2(m-3)\rangle\\
&\oplus(\tbinom{m-1}{2}-1)\langle r_2\rangle \ominus \langle r_2(m-1)(m-2)(m-3)\rangle \oplus \langle 2r_2(m-3)\rangle \ominus \langle 2r_2(m-2)\rangle\\
=\;&\langle r_0\tbinom{m}{2}\rangle \oplus \langle 2r_2\rangle \oplus (m-1)\langle r_2\rangle \ominus (m-1)\langle r_2(m-2)\rangle\\
&\oplus (\tbinom{m-1}{2}-1)\langle r_2\rangle \oplus \langle r_2(m-2)\rangle \ominus \langle 2r_2(m-1)\rangle \ominus \langle 2r_2(m-2)\rangle\\
=\;&\langle r_0\tbinom{m}{2}\rangle \oplus \langle 2r_2\rangle \oplus (\tbinom{m}{2}-1)\langle r_2\rangle \ominus m\langle r_2(m-2)\rangle\\
&\oplus 2\langle r_2(m-2)\rangle \ominus \langle 2r_2(m-1)\rangle \ominus \langle 2r_2(m-2)\rangle.
\end{aligned}$$

This finishes the proof, since $2\langle r_2(m-2)\rangle \ominus \langle 2r_2(m-2)\rangle = \langle 2r_2(m-2)\rangle$. ■

Proof of Theorem 3.2. By definition $\tau = y - x$, so **(1)** is obvious. Let H denote the $v \times b$ incidence matrix of the triangular design. Since $\mathcal{T}_{m-1}^c$ is an induced subgraph of $\mathcal{T}_m^c$, H has a $v \times v$ submatrix $\tilde{H}$ satisfying

$$\tilde{H}^\top \tilde{H} = (k-x)I + \tau T_{m-1}^c + xJ = \mathbb{T}_{m-1}(k^2, \tau, \tau(m-2)).$$

So $\det \tilde{H}^\top \tilde{H} = k^2\tau^{m-2}(\tau(m-2))^{\binom{m-2}{2}-1}$, hence $(m-2)^{\binom{m}{2}}\tau^{\binom{m+1}{2}} = \square$ which proves **(2)**. Moreover, $\mathbb{T}_{m-1}(k^2, \tau, \tau(m-2))$ is decomposable, so by Theorem 3.1 and **(1)** of Lemma 2.1 we find

$$\begin{aligned}
&\langle\tbinom{m-1}{2}\rangle \oplus (m-1)\langle\tau(m-3)\rangle \ominus \langle\tau(m-1)(m-3)\rangle \oplus \langle 2\tau(m-2)\rangle\\
&\oplus \tfrac{1}{2}m(m-3)\langle\tau(m-2)\rangle \ominus (m-1)\langle\tau(m-2)(m-3)\rangle \oplus \langle 2\tau(m-2)(m-3)\rangle \ominus \langle 2\tau\rangle\\
&= 0.
\end{aligned}$$

By **(2)** of Lemma 2.1 we have

$$\begin{aligned}
\langle 2\tau(m-2)\rangle \oplus \langle 2\tau(m-2)(m-3)\rangle \ominus \langle 2\tau\rangle &= \langle 2\tau(m-3)\rangle,\\
\langle\tau(m-3)\rangle \ominus \langle\tau(m-2)(m-3)\rangle &= \langle\tau(m-2)\rangle \ominus \langle\tau\rangle,\\
\langle 2\tau(m-3)\rangle \ominus \langle\tau(m-1)(m-3)\rangle &= \langle 2\tau(m-1)\rangle \ominus \langle\tau\rangle.
\end{aligned}$$

Hence

$$\langle\tbinom{m-1}{2}\rangle \oplus (\tbinom{m}{2}-1)\langle\tau(m-2)\rangle \oplus \langle 2\tau(m-1)\rangle \ominus m\langle\tau\rangle = 0,$$

proving **(3)**. ■

Proof of Corollary 3.3. We distinguish eight cases depending on the value of m mod 8. First we simplify the conditions **(2)** and **(3)** for these cases by use of Lemma 2.1. We find

$$\begin{array}{lll}
m \equiv 0 \bmod 8: & & \langle 2\tau(m-1)\rangle \oplus \langle 2(m-1)(m-2)\rangle = \langle \tau(m-2)\rangle, \\
m \equiv 1 \bmod 8: & \tau = \square, & \langle m-2\rangle \oplus \langle 2\rangle = \langle 2(m-2)\rangle, \\
m \equiv 2 \bmod 4: & \tau(m-2) = \square, & 2\langle m-1\rangle = 0, \\
m \equiv 3 \bmod 8: & m-2 = \square, & \langle 2(m-1)\rangle \oplus \langle 2\tau(m-1)\rangle = \langle \tau\rangle, \\
m \equiv 4 \bmod 8: & & \langle 2\tau(m-1)\rangle \oplus \langle 2(m-1)(m-2)\rangle \oplus \langle \tau(m-2)\rangle = 0, \\
m \equiv 5 \bmod 8: & \tau = \square, & \langle m-2\rangle \oplus \langle 2(m-2)\rangle = \langle 2\rangle, \\
m \equiv 7 \bmod 8: & m-2 = \square, & \text{irrelevant, since 5 is not a square } \bmod 8.
\end{array}$$

Now apply Lemmas 2.1 to 2.6. ∎

5. Known Non-Existence Results

The aim of this section is to show that for triangular designs Theorem 3.2 covers all other known non-existence results (at least the ones known to us). Several papers are written about restrictions on quasi-symmetric designs. Results relevant to triangular designs are in [1], [3], [4], [5], [22]. In this section we assume that p is an odd prime and $p|\tau$. (Remember that $\tau = y - x = \frac{a(m-a-1)}{2(m-3)}$.) Therefore $p|a$ or $p|(m-a-1)$. We may assume that $p|a$, for otherwise we consider the complementary design. Notice that $p|a$ and $p\nmid(m-3)$ implies $p|x$, $p|r$, $p|k$, $p|\lambda$ and $p|\tau$. We will frequently use the formula

$$r - \lambda = \tau(m-2). \tag{5}$$

In Corollary 3 of [1] the following result is proved:

LEMMA 5.1 *Consider a triangular design. Suppose p is an odd prime such that $p|\tau^*$ and $p\nmid m(m-1)(m-2)$. Then*

(i) $m \equiv 0, 3 \bmod 4$.

(ii) If $m \equiv 0, 3 \bmod 8$ *then* $\left(\frac{v}{p}\right) = 1$.

(iii) If $m \equiv 4 \bmod 8$ *then* $\left(\frac{-v}{p}\right) = 1$.

Claim. The restrictions given in Lemma 5.1 follow from Theorem 3.2.

Proof: The condition $p|\tau^*$ implies that $\tau \neq \square$. Since $p\nmid m-2$, also $\tau(m-2) \neq \square$. But if $m \equiv 1 \bmod 4$, then $\tau = \square$, and if $m \equiv 2 \bmod 4$, then $\tau(m-2) = \square$, by Corollary 3.3. Therefore we conclude (i). Next, by considering in (i), (iv) and (v) of Corollary 3.3 the Diophantine equations modulo p, we find (ii) and (iii). ∎

Note that, unlike Bagchi, we did not need that $p\nmid m$, so the second condition for p can be replaced by $p\nmid v$. In [5], Calderbank gives some restrictions for the existence of quasi–symmetric designs. The statement restricted to triangular designs reads:

LEMMA 5.2 *Suppose p is an odd prime and $p|\tau$. Then either*

(i) $r \equiv \lambda \bmod p^2$,

(ii) v *is odd*, $k \equiv x \equiv r \equiv \lambda \equiv 0 \bmod p$ *and* $\left(\frac{v}{p}\right) = -1$,

(iii) v *is odd*, $k \equiv x \equiv r \equiv \lambda \equiv 0 \bmod p$ *and* $\left(\frac{v}{p}\right) = \left(\frac{-1}{p}\right)^{(v-1)/2} = 1$.

Claim. The restrictions given in Lemma 5.2 follow from Theorem 3.2.

Proof: We assume that $p|a$. If $p|(m-2)$ then $p^2|(r-\lambda)$ by Formula 5. If $p|(m-a-1)$ then $p^2|\tau$ and hence $p^2|(r-\lambda)$. All these cases correspond to Calderbank's case (i). Now we assume that $\operatorname{ord}_p(\tau) = 1$ and $p \nmid v$. Now we apply Lemma 5.1. Hence $m \equiv 0, 3 \bmod 4$, which implies that v is odd. Furthermore

$$\left(\frac{(-1)^{(v-1)/2}v}{p}\right) = 1,$$

hence

$$\left(\frac{-1}{p}\right)^{(v-1)/2} = \left(\frac{v}{p}\right).$$

If $m \equiv 0, 3 \bmod 8$ then $v \equiv 1 \bmod 4$. This corresponds to Calderbank's case (iii). If $m \equiv 4 \bmod 8$ then $v \equiv 3 \bmod 4$. The case $(\frac{v}{p}) = -1$ corresponds to case (ii), while the case $(\frac{v}{p}) = 1$ corresponds to case (iii). ■

From Theorem 5.1 of Blokhuis and Calderbank [3], it follows that triangular designs satisfy ($\operatorname{ord}_p(n)$ is the largest integer k such that p^k divides n):

LEMMA 5.3 *Let p be an odd prime. Suppose* $\operatorname{ord}_p(\tau) = e$ *and e is odd. Then either*

(i) $r \equiv \lambda \bmod p^{e+1}$,

(ii) v *odd*, $\operatorname{ord}_p(x)$ *is odd and* $\left(\frac{(-1)^{(v-1)/2}(v-x)^*}{p}\right) = 1$,

(iii) v *odd*, $\operatorname{ord}_p(x)$ *is even and* $\left(\frac{(-1)^{(v-1)/2}x^*}{p}\right) = 1$.

Claim. The restrictions given in Lemma 5.3 follow from Theorem 3.2.

Proof: If $p|(m-2)$ then $\operatorname{ord}_p(r-\lambda) > e$, which is Blokhuis and Calderbank's case (i). Hence we will assume that $p \nmid (m-2)$. This implies (by Corollary 5.1) that $\operatorname{ord}_p(\tau) = \operatorname{ord}_p((m-2)\tau) = e$, which eliminates the cases $m \equiv 1, 2 \bmod 4$. Hence v is odd. Let $\operatorname{ord}_p(a) = \alpha$, $\operatorname{ord}_p(m-a-1) = \beta$ and $\operatorname{ord}_p(m-3) = \gamma$. Then we have $\alpha + \beta - \gamma = e$.

If $\gamma > 0$ then $\alpha\beta = 0$ and if $\alpha\beta > 0$ then $\gamma = 0$. We distinguish several cases:

(i) If $\gamma > 0$ then either $p|a$ or $p|(m-a-1)$. We may assume that $p|(m-a-1)$. Now $a \equiv m-1 \equiv 2 \bmod p$. Hence $x \equiv 1 \bmod p$. But also $v \equiv 1 \bmod p$. Hence

$$\left(\frac{(-1)^{(v-1)/2}x^*}{p}\right) = \left(\frac{(-1)^{(v-1)/2}v}{p}\right) = 1$$

by Lemma 5.1.

(ii) If $\alpha > \beta$ and α is odd (hence β is even) then $v - x \equiv v \bmod p^\alpha$ and $\mathrm{ord}_p(v) = \beta$. It is easy to verify that

$$\left(\frac{(-1)^{(v-1)/2}v^*}{p}\right) = 1.$$

(iii) If $\alpha > \beta$ and α is even (hence $\beta > 0$) then $a \equiv m-1 \bmod p^\alpha$, and hence $x^* \equiv v^* \bmod p$.

(iv) If $\alpha < \beta$ then interchange a and $m-a-1$. Now we get case (ii) or case (iii). ∎

For the case of $p = 2$ we found two relevant results, one by Calderbank [4] and one by Skinner [22]. Calderbank's result (Theorem 1 in [4]) restricted to triangular designs gives.

LEMMA 5.4 *Assume τ is even. Then either*

(i) $r \equiv \lambda \bmod 4$,

(ii) *x is even,* $k \equiv 0 \bmod 4$ *and* $v \equiv \pm 1 \bmod 8$,

(iii) *x is odd,* $k \equiv v \bmod 4$ *and* $v \equiv \pm 1 \bmod 8$.

Claim. The restrictions given in Lemma 5.4 also follow from Theorem 3.2.

Proof: If m is even then (since τ is even) $4|\tau(m-2)$ hence (i) holds. If $m \equiv 1 \bmod 4$ then τ is a square and again case (i) is satisfied. If $m \equiv 3 \bmod 16$ then $v \equiv 1 \bmod 8$ and τ is even implies that $a \equiv 0, 2 \bmod 8$. If $a \equiv 0 \bmod 8$ then we have case (ii), if $a \equiv 2 \bmod 8$ then we have case (iii). If $m \equiv 11 \bmod 16$ then τ has to be odd (see Corollary 3.3). This agrees with Calderbank's result. ∎

The result by Skinner [22] is an extension of the previous result and has the following consequence for triangular designs.

LEMMA 5.5 *Suppose* $\mathrm{ord}_2(\tau) = e$ *and e is odd. If* $\mathrm{ord}_2(r-\lambda) = e$ *then* $v \equiv 1 \bmod 8$ *and* $k \equiv 0, 1 \bmod 4$

Claim. The restrictions given in Lemma 5.5 follow from Theorem 3.2.

Proof: $\mathrm{ord}_2(r-\lambda) = \mathrm{ord}_2(\tau)$ implies that m is odd (see Formula 5). Since $\mathrm{ord}_2(\tau)$ is odd, $\tau \neq \square$, so $m \not\equiv 1 \bmod 4$. Hence $m \equiv 3 \bmod 8$. Corollary 3.3 implies that $m \equiv 3 \bmod 16$. Hence $v \equiv 1 \bmod 8$. Moreover, since $a(m-a-1) = 2\tau(m-3)$, $\mathrm{ord}_2(a(m-a-1)) \geq 6$. So without loss of generality $8|a$ and hence $k = a(m-2)/2 \equiv 0 \bmod 4$. ■

If $a = 2$, triangular designs are 2-$(\binom{m-1}{2}, m-2, 2)$ designs. These designs are quasi-residual for (symmetric) 2-$(\binom{m}{2}+1, m, 2)$ designs (better known as biplanes). By Hall and Connor [14] such a design is actually a residual design, which means that it exists if and only if the corresponding biplane exists. Thus the Bruck-Ryser-Chowla conditions for biplanes give the following conditions for triangular designs.

LEMMA 5.6 *Suppose $a = 2$, then*

(i) if $m \equiv 2, 3, 6 \bmod 8$, then $m-2 = \square$,

(ii) if $m \equiv 0, 1 \bmod 8$, then $m-2 \in \mathcal{N}_2$,

(iii) if $m \equiv 4, 5 \bmod 8$, then $m-2 \in \mathcal{N}_{-2}$,

(iv) $m \not\equiv 7 \bmod 8$.

Claim. The restrictions above and those given by Theorem 3.2 for $a = 2$ are the same.

Proof: If $a = 2$ then $\tau = 1 = \square$, and (2) and (3) of Theorem 3.2 become

$$(m-2)^{\binom{m}{2}} = \square,$$
$$(\tbinom{m}{2} - 1)\langle m-2\rangle \oplus \langle 2(m-2)\rangle \oplus \langle 2\rangle = 0.$$

By Lemma 2.2, 2.3 and 2.6, we find the above formulas. ■

Note that we only used that $\tau = \square$. Therefore the conditions of Lemma 5.6 are precisely the conditions of Theorem 3.2 in case $\tau = \square$.

Unfortunately, but not suprisingly, Theorem 3.2 gives no new non-existence results for biplanes. We don't know of any other results than the ones mentioned here that give non-existence conditions for triangular designs. We have seen that Theorem 3.2 covers all these results. But the theorem is stronger. For instance the case $m = 24$, $a = 9$ is excluded by (3) of Theorem 3.2 (see the next section), but by none of the above results.

6. Some Parameter Sets

In this last section we discuss some special sets of parameters for triangular designs.

The case $a = 2$

As remarked before, these are the residual designs of biplanes. Biplanes have been constructed for $m = 4, 5, 6, 9, 11$ and 13. These, and their complements provide the only known examples of triangular designs. The smallest value for which existence of a biplane is not known is $m = 16$. This is also the smallest unknown triangular design (see tabel below).

The case $m \leq 100$ and $2 < a < m/2$

Remember that we do not lose generality by requiring $a < m/2$. We computed all feasible parameter sets for triangular designs in this range. It turned out that 48 values of (a, m) survived condition (**1**) of Theorem 3.2, and 16 survived (**1**) and (**2**). These 16 are given in the table below.

m	a	v	k	λ	x	y	τ	p
† 24	9	253	99	42	36	39	3	11
27	8	325	100	33	28	31	3	
33	12	496	186	74	66	70	4	
36	11	630	198	62	55	59	4	
48	20	1081	460	204	190	196	6	
51	18	1225	441	165	153	159	6	
† 60	21	1711	609	224	210	217	7	29
66	9	2080	288	41	36	40	4	
† 68	15	2211	495	114	105	111	6	11
72	23	2485	805	268	253	261	8	
73	30	2556	1065	456	435	444	9	
† 80	35	3081	1365	620	595	605	10	3
81	26	3160	1027	342	325	334	9	
83	32	3321	1296	518	496	506	10	
† 88	17	3741	731	146	136	143	7	7
† 96	33	4465	1551	550	528	539	11	11

The parameter sets indicated with † are excluded by (**3**) of Theorem 3.2. For these parameters it is indicated modulo which prime p the Diophantine equation is not satisfied. It seems worthwhile to remark that, unlike in most non-existence results (see the previous section), the prime that works is often not a divisor of τ. Thus, only 10 possible parameters with $m \leq 100$ and $2 < a < m/2$ are left over.

Many feasible parameter sets for triangular designs are excluded by Theorem 3.2. But on the other hand, some infinite series survive. We shall give some examples. First observe that from the definition of τ we derive for $2 < a < m - 3$

$$m = a + 2\tau + 1 + \frac{4\tau(\tau - 1)}{a - 2\tau}. \tag{6}$$

Therefore $a - 2\tau$ must be a divisor of $4\tau(\tau - 1)$.

The case $a = 2\tau + 1$

Then $m = 4\tau^2 + 2$, and hence $m \equiv 2 \bmod 4$. Notice that $m - 2 = 4\tau^2$ is a square. Since by Theorem 3.2 $\tau(m-2) = \square$, we conclude that $\tau = \square$. Thus we find the following infinite sequence of parameters satisfying all our conditions.

τ	a	m
u^2	$2u^2 + 1$	$4u^4 + 2$

The case $a = 3\tau - 1$

This implies that $m = 9\tau$. We consider the possible values of m mod 8.

0: $\tau = 8u$. $m = 72u$ and $a = 24u - 1$ satisfy Corollary 3.3 ($X = 3$, $Y = 1$ and $Z = 1$).

1: $\tau = (2u+1)^2$. m and a satisfy Corollary 3.3 (as a consequence of Lemma 2.6).

2,6: Impossible! ($\tau(9\tau - 2) = \square$ has no integral solutions.)

3: $m - 2 = q^2$ implies $q \equiv \pm 5 \bmod 18$. Now $\tau = \frac{1}{9}(q^2+2)$, $m = q^2+2$ and $a = \frac{1}{3}(q^2-1)$ satisfy Corollary 3.3 with $X = 3$, $Y = q$ and $Z = 1$.

4: Condition (3) of Theorem 3.2 gives $\langle 2\tau(9\tau-1)\rangle \oplus \langle 2(9\tau-1)(9\tau-2)\rangle \oplus \langle \tau(9\tau-2)\rangle = 0$. This is equivalent with $2\langle\tau\rangle \oplus 2\langle 9\tau - 2\rangle = 0$. Since $\gcd(\tau, 9\tau - 2) = 2$ both terms of the equation have to be zero. Hence $\tau, 9\tau - 2 \in \mathcal{N}_{-1}$.

5,7: Impossible, since 5 is not a square mod 8.

We find the following three series of possible values for a and m in case $a = 3\tau - 1$.

τ	a	m
$8u$	$24u - 1$	$72u$
$(2u+1)^2$	$3(2u+1)^2 - 1$	$9(2u+1)^2$
$36u^2 \pm 20u + 3$	$108u^2 \pm 60u + 8$	$(18u \pm 5)^2 + 2$

The case $a = 4\tau$

Then $m = 8\tau - 1$, which is impossible by Corollary 3.3.

The case $\tau = u^2$

If $\tau = u^2$, then the divisibility condition in Formula 6 reads $a - 2u^2$ divides $4(u-1)u^2(u+1)$. In this case the conditions of Theorem 3.2 are as given in Lemma 5.6, and many parameters survive.

The case $\tau = \binom{u}{2}$

If $\tau = \binom{u}{2}$, the divisibility in Formula 6 is $a - u(u-1)$ divides $(u+1)u(u-1)(u-2)$. Many feasible parameters satisfy our conditions. One of these cases is given below. Notice that $m - 2 = (2u-1)^2$ is a square. The Diophantine equation of Corollary 3.3 is satisfied, by $X = 4$, $Y = 2$ and $Z = 1$.

τ	a	m
$\binom{u}{2}$	$2(u-1)^2$	$4u^2 - 4u + 3$

Finally we remark that we expect that no triangular design with $2 < a < m - 3$ will ever be found. But we don't have enough evidence to conjecture that they don't exist.

References

1. Bagchi, B. 1992. On quasi-symmetric designs. *Designs, Codes and Cryptography* 2:69–79.
2. Beth, T., Jungnickel, D., and Lenz, H. 1986. *Design Theory*. Cambridge University Press, Cambridge.
3. Blokhuis, A., and Calderbank, R. 1992. Quasi-symmetric designs and the Smith normal form. *Designs, Codes and Cryptography* 2:189–206.
4. Calderbank, A. R. 1987. The application of invariant theory to the existence of quasi-symmetric designs. *J. Combin. Theory A* 44:94–109.
5. Calderbank, A. R. 1988. Geometric invariants for quasi-symmetric designs. *J. Combin. Theory A* 47:101–110.
6. Cameron, P. J., and van Lint, J. H. 1991. *Designs, Graphs, Codes and their Links*. Cambridge University Press, Cambridge.
7. Cassels, J. W. S. 1978. *Rational Quadratic Forms*. Academic Press, London.
8. Chang, L. C. 1959. The uniqueness and non-uniqueness of the triangular association scheme. *Sci. Record Peking Math.* 3:604–613.
9. Connor, W. S. 1952. On the structure of balanced incomplete block designs. *Ann. Math. Stat.* 23:57–71.
10. Conway, J. H., and Sloane, N. J. A. 1988. *Sphere Packings, Lattices and Groups*. Springer-Verlag, New York.
11. Coster, M. J. 1994. *Quadratic Forms in Design Theory*, Research Memorandum 635, Tilburg University.
12. Goethals, J. M., and Seidel, J. J. 1970. Strongly regular graphs derived from combinatorial designs. *Can. J. Math.* 22:597–614.
13. Haemers, W. H. 1992. A non-existence result for quasi-symmetric designs. *Sankhyā: The Indian J. Stat.* **54** (Proceedings R. C. Bose Memorial Conference, Calcutta 1988), 189–190.
14. Hall, M., and Connor, W. S. 1954. An imbedding theorem for balanced incomplete block designs. *Can. J. Math.* 6:35–41.
15. Hardy, G. H., and Wright, E. M. 1983. *An Introduction to the Theory of Numbers*, fifth edition. Oxford University Press, Oxford.
16. Hoffman, A. J. 1960. On the uniqueness of the triangular association scheme. *Ann. Math. Stat.* 31:492–497.

17. Lander, E. S. 1983. *Symmetric Designs: An Algebraic Approach*. Cambridge University Press, Cambridge.
18. Mordell, L. J. 1969. *Diophantine Equations* Academic Press, London, New York.
19. Shrikhande, M. S., and Sane, S. S. 1991. *Quasi-symmetric Designs*. Cambridge University Press, Cambridge.
20. Shrikhande, S. S., and Bhagwandas. 1965. Duals of incomplete block designs. *J. Indian Stat. Ass.* 3:30–37.
21. Shrikhande, S. S., Raghavarao, D., and Tharthare, S. K. 1963. Non-existence of some partially balanced incomplete block designs. *Can. J. Math.* 15:686–701.
22. Skinner, C. M. 1993. Non-symmetric 2-designs modulo 2. *Designs, Codes and Cryptography* 3:63–68.